REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
01-08-2017

2. REPORT TYPE
Final Report

3. DATES COVERED (From - To)
24-Aug-2012 - 23-Aug-2017

4. TITLE AND SUBTITLE
Final Report: Hierarchical Trust Management of COI in Heterogeneous Mobile Networks

5a. CONTRACT NUMBER
W911NF-12-1-0445

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS
Ing-Ray Chen

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Virginia Polytechnic Institute & State Unive
North End Center, Suite 4200
300 Turner Street, NW
Blacksburg, VA 24061 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
61654-CS.30

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES
UU	UU	UU	UU	

19a. NAME OF RESPONSIBLE PERSON
Ing Ray Chen

19b. TELEPHONE NUMBER
703-538-8376

RPPR Final Report
as of 17-Nov-2017

Agency Code:

Proposal Number: 61654CS
Agreement Number: W911NF-12-1-0445
INVESTIGATOR(S):

Name: Ing Ray Chen
Email: irchen@vt.edu
Phone Number: 7035388376
Principal: Y

Name: Jin-hee Cho
Email: jin-hee.cho.civ@mail.mil
Phone Number: 3013940492
Principal: N

Organization: **Virginia Polytechnic Institute & State University**
Address: North End Center, Suite 4200, Blacksburg, VA 240610001
Country: USA
DUNS Number: 003137015
EIN: 546001805
Report Date: 23-Nov-2016
Date Received: 01-Aug-2017
Final Report for Period Beginning 24-Aug-2012 and Ending 23-Aug-2017
Title: Hierarchical Trust Management of COI in Heterogeneous Mobile Networks
Begin Performance Period: 24-Aug-2012
End Performance Period: 23-Aug-2017
Report Term: 0-Other
Submitted By: Ing Ray Chen
Email: irchen@vt.edu
Phone: (703) 538-8376
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 3
STEM Participants: 4

Major Goals: There are three major goals:

1. Scalability, Reconfigurability, Survivability and Intrusion Tolerance for Community of Interest (COI) Applications – Our proposed COI trust management protocol will leverage COI hierarchical management (COI-HM) for scalability and reconfigurability following the Army command chain of commander->leader->COI members. Under COI-HM, a COI is divided into multiple subtask groups to accomplish a mission. Each subtask group would be governed by a subtask group leader (SGL) dynamically appointed by the COI commander responsible for relaying commands from the commander to the COI group members in the subtask group, and filtering messages sent by COI members in the same subtask group to COI members located in other subtask groups. COI members in one subtask group may be reassigned to another subtask group for tactical reasons, thus triggering registration/deregistration actions to the subtask group leaders, as well as secret key rekeying operations to maintain the hierarchical structure and to ensure secure group communication functionality. This hierarchical management structure is generic and can be applied to various mission scenarios. Subtask groups may be physically co-located or separated. A node may be assigned to one or more subtasks, depending on node properties (e.g., manned or unmanned) and subtask group characteristics (functionality, difficulty, urgency, importance, risk, size, and composition). Thus, a node's mobility model reflects its assignment, de-assignment or reassignment to subtask groups, as well as its movement pattern moving around the subtask groups it is assigned to. Here we note that in military applications, very frequently a COI consists of heterogeneous nodes with vastly different levels of functionality, capacity and resources. A SGL is presumably a higher-capacity node and would be assigned, de-assigned, or reassigned dynamically by the COI-commander to lead a subtask group. Despite providing scalability and reconfigurability, COI-HM does not provide tolerance against node compromises and collusion as there is no mechanism to defend against inside attackers or malicious nodes. Existing intrusion detection system (IDS) techniques based on anomaly or pattern-based detection are either centralized (especially for wired networks) which creates a single point of failure, or too complex for distributed execution in heterogeneous mobile networks at runtime. In this research work, we propose COI dynamic hierarchical trust management (COI-HiTrust) for intrusion tolerance and survivability extending from our ONR-sponsored work on trust management for mobile ad hoc networks (MANETs). As COI-HiTrust runs on top of COI-HM, it also achieves scalability and reconfigureability since nodes will only interact with peers in the same subtask group and do not

assess trust about every node in the network.

2. Dynamic Hierarchical Trust Management – Recognizing that COI nodes very likely will involve human operators controlling communication devices (e.g., device-carried soldiers, and vehicles operated by human operations), we will design COI-HiTrust to explore, compose and measure trust in a way humans estimate with their cognition, e.g., competence is about task performance, intimacy is about comfortableness of having close nodes in the same mission, and honesty is about integrity rather than competence, to properly characterize trust for Army COI applications. We will design COI-HiTrust to be dynamically reconfigurable and capable of adjusting trust parameters for protocol execution in response to dynamically changing environments (e.g., in response to increasing misbehaving node populations or evolving node density because of node failure, eviction, mobility or disconnection/reconnection) to maximize application performance.

3. Applications to Real-World Army COI Applications - We will design a modeling and analysis tool to facilitate application of COI-HiTrust to hierarchically structured Army COI applications in (service-oriented) mobile ad hoc networks (MANETs), Internet of Things (IoT) systems, mobile wireless sensor networks (MWSNs), delay tolerate networks (DTNs), and mobile cyber physical systems (MCyPhs) in which COI mobile nodes collaborate to accomplish a mission despite the presence of malicious, erroneous, partly trusted, uncertain and incomplete information.

Accomplishments: See the pdf document uploaded

Training Opportunities: Nothing to Report

Results Dissemination: The major venue for results dissemination is publication through major IEEE/ACM conferences/journals. This ARO sponsored research has resulted in 23 publications (see Accomplishments uploaded), including 7 IEEE Transactions publications, all acknowledging this ARO grant.

Honors and Awards: Both PIs, Dr. Ing-Ray Chen and Dr. Jin-Hee Cho, received the IEEE Communications Society William R. Bennett Prize in the field of Communications Networking in 2015, and the U.S. Army Research Laboratory (ARL) Publication Award in 2016. In addition, Jin-Hee Cho received the prestigious Presidential Early Career Awards for Scientists and Engineers (PECASE) Award in 2016.

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Ing-Ray Chen
Person Months Worked: 10.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Jin-Hee Cho
Person Months Worked: 5.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

ARTICLES:

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 5-Submitted
Journal: IEEE Transactions on Parallel and Distributed Systems
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Trust and Risk Managementfor Task Assignment in Tactical Networks
Authors:
Keywords: Trust, risk, composite trust metric, task assignment, tactical network, mission completion, task, risk-seeking, risk-neutral, risk-averse.
Abstract: Resource or task assignment problems have been extensively studied in tactical network environments as efficient and effective resource allocation is the key to successful mission completion. Existing works on asset-task assignment problems are based only on the best match between functionalities of a node and requirements of a task. In this work, we propose a composite trust-based task assignment protocol that can maximize mission completion ratio based on the tradeoff between trust and risk. Leveraging the core concept of trust as the wiliness to take a risk, the proposed protocol selects qualified nodes for a given task while meeting an acceptable risk level for successful task execution. Given a mission consisting of dynamic multiple tasks, we model each task in terms of importance, urgency, and difficulty characteristics and use them for the member selection process. In addition, we model a node's risk behavior (risk-seeking, risk-neutral, and risk-averse) and investigate its impa
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 5-Submitted
Journal: IEEE Transactions on Parallel and Distributed Systems
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing
Authors:
Keywords: Delay tolerant networks, dynamic trust management, secure routing, performance analysis, design and validation.
Abstract: Delay tolerant networks (DTNs) are characterized by high end-to-end latency, frequent disconnection, and opportunistic communication over unreliable wireless links. In this paper, we design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. We develop a novel model-based methodology for the analysis of our trust protocol and validate it via extensive simulation. Moreover, we address dynamic trust management, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. We perform a comparative analysis of our proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. The results demonstrate that our protocol is able to deal with selfish behaviors and is resilient against trust-rel
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 5-Submitted
Journal: IEEE Transactions on Network and Service Management
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Adaptive Trust Management for Social Internet of Things
Authors:
Keywords: Trust management, Internet of things, social networking, performance analysis, adaptive control, security.
Abstract: An Internet of Things (IoT) system aims to connect "things" in both physical world and cyberspace, which raises great challenges to trust management with respect to heterogeneity, scalability, and system dynamics. We propose and analyze the design notion of adaptive trust management for social IoT environments in which social relationships evolve dynamically among the owners of IoT devices. We formally prove the convergence, accuracy, and resiliency properties of our adaptive trust management protocol against trust attacks. Moreover, we reveal the design tradeoff between trust convergence vs. trust fluctuation. With our adaptive trust management protocol, a social IoT application can adaptively choose the best trust parameter settings in response to changing IoT social conditions such that not only trust assessment is accurate but also the application performance is maximized. The utility of adaptive trust management is demonstrated by a trust-based service composition application in s
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Ad Hoc Networks
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.adhoc.2013.05.004
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: On the tradeoff between altruism and selfishness in MANET trust management
Authors:
Keywords: altruism, selfishness, demand and pricing theory, mobile ad hoc networks, trust management.
Abstract: Mobile ad hoc and sensor networks may consist of a mixture of nodes, some of which may be considered selfish due to a lack of cooperativeness in providing network services such as forwarding packets. In the literature, existing trust management protocols for mobile ad hoc networks advocate isolating selfish nodes as soon as they are detected. Further, altruistic behaviors are encouraged with incentive mechanisms. In this paper, we propose and analyze a trust management protocol for group communication systems where selfish nodes exist and system survivability is highly critical to mission execution. Rather than always encouraging altruistic behaviors, we consider the tradeoff between a node's individual welfare (e.g., saving energy to prolong the node lifetime) versus global welfare (e.g., achieving a given mission with sufficient service availability) and identify the best design condition of this behavior model to balance selfish vs. altruistic behaviors. With the system lifetime and
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Parallel and Distributed Systems
Publication Identifier Type: DOI Publication Identifier: 10.1109/TPDS.2013.116
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing
Authors:
Keywords: Delay tolerant networks, dynamic trust management, secure routing, performance analysis, design and validation.
Abstract: Delay tolerant networks (DTNs) are characterized by high end-to-end latency, frequent disconnection, and opportunistic communication over unreliable wireless links. In this paper, we design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. We develop a novel model-based methodology for the analysis of our trust protocol and validate it via extensive simulation. Moreover, we address dynamic trust management, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. We perform a comparative analysis of our proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. The results demonstrate that our protocol is able to deal with selfish behaviors and is resilient against trust-rel
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Network and Service Management
Publication Identifier Type: DOI Publication Identifier: 10.1109/TNSM.2013.043013.120282
Volume: 10 Issue: 2 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks
Authors:
Keywords: Heterogeneous wireless sensor networks; multipath routing; intrusion detection; reliability; security; energy conservation.
Abstract: In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detec
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: N **Publication Status:** 5-Submitted
Journal: Milcom
Publication Identifier Type: Publication Identifier:
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Trust-based Service Composition and Binding for Tactical Networks with Multiple Objectives
Authors:
Keywords: Trust, risk, service composition, tactical networks, multi-objective optimization.
Abstract: Tactical networks often make decisions in selecting service providers to meet service requirements of a tactical mission operation while facing lack of resources and high security vulnerability. We consider a tactical environment in which nodes provide services to support various operations and/or may request services to support the operations as well. We formulate the problem of service composition and service binding as a multi-objective optimization (MOO) problem. The MOO problem is essentially a node-to-service assignment problem such that by dynamically formulating service composition, and selecting the right nodes to provide requested services, the tactical network can support concurrent operations while achieving multiple system objectives such as minimizing the service cost, while maximizing the quality of service (QoS) and quality of information (QoI). We develop a trust-based service composition and binding protocol. By means of a novel iterative solution technique utilizing
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Ad Hoc Networks
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.adhoc.2014.02.005
Volume: 19 Issue: 0 First Page #: 59
Date Submitted: Date Published:
Publication Location:
Article Title: Trust management in mobile ad hoc networks for bias minimization and application performance maximization
Authors:
Keywords: Trust management, Mobile ad hoc networks,Trust bias minimization, Model-based analysis, Application-level trust optimization, Reliability assessment.
Abstract: Trust management for mobile ad hoc networks (MANETs) has emerged as an active research area as evidenced by the proliferation of trust/reputation protocols to support mobile group based applications in recent years. In this paper we address the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization. By means of a novel model-based approach to model the ground truth status of mobile nodes in MANETs as the basis for design validation, we identify and validate the best trust protocol settings under which trust bias is minimized and application performance is maximized. We demonstrate the effectiveness of our approach with an integrated social and quality-of-service (QoS) trust protocol (called SQTrust) with which we identify the best trust aggregation setting under which trust bias is minimized despite the presence of malicious nodes performing slandering attacks. Furthermore, using a missio
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: ACM Transactions on Sensor Networks
Publication Identifier Type: DOI Publication Identifier: 10.1145/2700830
Volume: 11 Issue: 3 First Page #: 47
Date Submitted: Date Published:
Publication Location:
Article Title: Integrated Intrusion Detection and Tolerance in Homogeneous Clustered Sensor Networks
Authors:
Keywords: Wireless sensor networks, intrusion tolerance, intrusion detection, multisource multipath routing, security, reliability, timeliness.
Abstract: In this paper we propose and analyze dynamic redundancy management of integrated intrusion detection and tolerance for lifetime maximization of homogeneous clustered wireless sensor networks (WSNs). We take a holistic approach of integrating multisource and multipath routing for intrusion tolerance with majority voting for intrusion detection in our redundancy management protocol design. By dynamically controlling the redundancy level for both multisource multipath routing and voting-based intrusion detection with energy consideration, we identify the optimal redundancy level to be applied to maximize the WSN lifetime in response to changing environment conditions including node density, radio range, and node capture rate. We demonstrate the effectiveness of our integrated redundancy management protocol by a comparative analysis with a multisource multipath routing algorithm called AFTQC that considers only fault/intrusion tolerance.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Services Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSC.2014.2365797
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Trust Management for SOA-based IoT and Its Application to Service Composition
Authors:
Keywords: Trust management; Internet of things; social networks; service composition; SOA; performance analysis.
Abstract: A future Internet of Things (IoT) system will connect the physical world into cyberspace everywhere and everything via billions of smart objects. On the one hand, IoT devices are physically connected via communication networks. The service oriented architecture (SOA) can provide interoperability among heterogeneous IoT devices in physical networks. On the other hand, IoT devices are virtually connected via social networks. In this paper we propose adaptive and scalable trust management to support service composition applications in SOA-based IoT systems. We develop a technique based on distributed collaborative filtering to select feedback using similarity rating of friendship, social contact, and community of interest relationships as the filter. Further we develop a novel adaptive filtering technique to determine the best way to combine direct trust and indirect trust dynamically to minimize convergence time and trust estimation bias in the presence of malicious nodes performing oppo
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Reliability
Publication Identifier Type: DOI Publication Identifier: 10.1109/TR.2015.2406860
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems
Authors:
Keywords: Cyber physical systems, intrusion detection,redundancy engineering, mean time to failure, modeling andanalysis.
Abstract: In this paper, we develop an analytical model based on stochastic Petri nets to capture the dynamics between adversary behavior and defense for cyber physical systems. We consider several types of failures including attrition failure, pervasion failure, and exfiltration failure which can happen to a cyber physical system. Using a modernized electrical grid as an example, we illustrate the parameterization process. Our results reveal optimal design conditions, including the intrusion detection interval, and the redundancy level, under which the modernized electrical grid's mean time to failure is maximized. Further, there exists a design tradeoff between exfiltration failure, attrition failure, and pervasion failure when using redundancy to improve the overall system reliability.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Dependable and Secure Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TDSC.2015.2420552
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Trust-based Service Management for Social Internet of Things Systems
Authors:
Keywords: Trust management, Internet of things, social networking, performance analysis, adaptive control, security.
Abstract: A social Internet of Things (IoT) system can be viewed as a mix of traditional peer-to-peer networks and social networks, where "things" autonomously establish social relationships according to the owners' social networks, and seek trusted "things" that can provide services needed when they come into contact with each other opportunistically. We propose and analyze the design notion of adaptive trust management for social IoT systems in which social relationships evolve dynamically among the owners of IoT devices. We reveal the design tradeoff between trust convergence vs. trust fluctuation in our adaptive trust management protocol design. With our adaptive trust management protocol, a social IoT application can adaptively choose the best trust parameter settings in response to changing IoT social conditions such that not only trust assessment is accurate but also the application performance is maximized. We propose a table-lookup method to apply the analysis results dynamically and de
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Network and Service Management
Publication Identifier Type: DOI Publication Identifier: 10.1109/TNSM.2015.2441059
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks
Authors:
Keywords: Wireless sensor networks, selective capture, smart attack, multipath routing, intrusion tolerance, intrusion detection, MTTF.
Abstract: We propose and analyze adaptive network defense management for countering smart attack and selective capture which aim to cripple the basic data delivery functionality of a base station based wireless sensor net-work. With selective capture, the adversaries strategically capture sensors and turn them into inside attackers. With smart attack, an inside attacker is capable of performing random, opportunistic and insidious attacks to evade de-tection and maximize their chance of success. We develop a model-based analysis methodology with simulation val-idation to identify the best defense protocol settings under which the sensor network lifetime is maximized against selective capture and smart attack.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Ad Hoc Networks
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.adhoc.2015.05.004
Volume: 0 Issue: 0 First Page #: 0
Date Submitted: Date Published:
Publication Location:
Article Title: Hierarchical trust management of community of interest groups in mobile ad hoc networks
Authors:
Keywords: Hierarchical trust management; Community of interest groups; Intrusion detection
Abstract: In mission-critical applications deployed in mobile ad hoc networks, very frequently a commander will need to assemble and dynamically manage Community of Interest (COI) mobile groups to achieve the mission assigned despite failure, disconnection or compromise of COI members. In this paper, we present a dynamic hierarchical trust management protocol that can learn from past experiences and adapt to changing environment conditions (e.g., increasing misbehaving node population, evolving hostility and node density, etc.) to enhance agility and maximize application performance. With trust-based misbehaving node detection as an application, we demonstrate how our proposed COI trust management protocol is resilient to node failure, disconnection and capture events, and can help maximize application performance in terms of minimizing false negatives and positives in the presence of mobile nodes exhibiting vastly distinct QoS and social behaviors.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Services Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSC.2015.2491285
Volume: pp Issue: 99 First Page #: 1
Date Submitted: 8/28/16 12:00AM Date Published:
Publication Location:
Article Title: Trust-based Service Composition and Binding with Multiple Objective Optimization in Service-Oriented Mobile Ad Hoc Networks
Authors: Yating Wang, Ing-Ray Chen, Jin-Hee Cho, Ananthram Swami, Kevin Chan
Keywords: service-oriented ad hoc networks, service composition, trust management, multi-objective optimization.
Abstract: With the proliferation of fairly powerful mobile devices and ubiquitous wireless technology, we see a transformation from traditional mobile ad hoc networks (MANETs) into a new era of service-oriented MANETs wherein a node can provide and receive services. Requested services must be decomposed into more abstract services and then bound; we formulate this as a multi-objective optimization (MOO) problem to minimize the service cost, while maximizing the quality of service and quality of information in the service a user receives. The MOO problem is an SP-to-service assignment problem. We propose a multidimensional trust based algorithm to solve the problem. We carry out an extensive suite of simulations to test the relative performance of the proposed trust-based algorithm against a non-trust-based counterpart and an existing single-trust-based beta reputation scheme.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Services Computing
Publication Identifier Type: DOI Publication Identifier: 10.1109/TSC.2016.2587259
Volume: pp Issue: 99 First Page #: 1
Date Submitted: 8/28/16 12:00AM Date Published:
Publication Location:
Article Title: CATrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks
Authors: Yating Wang, Ing-Ray Chen, Jin-Hee Cho, Ananthram Swami, Yen-Cheng Lu, Chang-Tien Lu, Jeffrey T
Keywords: Trust, service-oriented ad hoc networks, logistic regression, recommendation attacks, statistical analysis.
Abstract: We propose a context-aware trust management model called CATrust for service-oriented ad hoc networks such as peer-to-peer and Internet of Things networks wherein a node can be a service requester or a service provider. The novelty of our design lies in the use of logistic regression to dynamically estimate trustworthiness of a service provider based on its service behavior patterns in response to context environment changes. We develop a recommendation filtering mechanism to effectively screen out dishonest recommendations even in extremely hostile environments in which the majority recommenders are dishonest. We demonstrate desirable convergence, accuracy, and resiliency properties of CATrust. We also demonstrate that CATrust outperforms contemporary peer-to-peer and Internet of Things trust models in terms of service trust prediction accuracy against collusion recommendation attacks.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Computer Communications
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.comcom.2015.08.001
Volume: 76 Issue: First Page #: 1
Date Submitted: 8/29/16 12:00AM Date Published: 2/1/16 5:00AM
Publication Location:
Article Title: A topic-focused trust model for Twitter
Authors: Liang Zhao, Ting Hua, Chang-Tien Lu, Ing-Ray Chen
Keywords: Trust management; Social networks; Twitter; Trustworthiness; Credibility
Abstract: Twitter is a crucial platform to get access to breaking news and timely information. However, due to questionable provenance, uncontrollable broadcasting, and unstructured languages in tweets, Twitter is hardly a trustworthy source of breaking news. In this paper, we propose a novel topic-focused trust model to assess trustworthiness of users and tweets in Twitter. Unlike traditional graph-based trust ranking approaches in the literature, our method is scalable and can consider heterogeneous contextual properties to rate topic-focused tweets and users. We demonstrate the effectiveness of our topic-focused trustworthiness estimation method with extensive experiments using real Twitter data in Latin America.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Ad Hoc Networks
Publication Identifier Type: DOI Publication Identifier: 10.1016/j.adhoc.2016.02.014
Volume: 44 Issue: First Page #: 58
Date Submitted: 8/29/16 12:00AM Date Published: 7/1/16 4:00AM
Publication Location:
Article Title: Trust threshold based public key management in mobile ad hoc networks
Authors: Jin-Hee Cho, Ing-Ray Chen, Kevin S. Chan
Keywords: Public key management; Mobile ad hoc networks; Trust; Private key; Public key; Certificate authority
Abstract: Public key management in mobile ad hoc networks (MANETs) has been studied for several decades. However, the unique characteristics of MANETs have imposed great challenges in designing a fully distributed public key management protocol under resource-constrained MANET environments. These challenges include no centralized trusted entities, resource constraints, and high security vulnerabilities. This work proposes a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. Instead of using hard security approaches, as in traditional security techniques, to eliminate security vulnerabilities, our work aims to maximize performance by relaxing security requirements based on the perceived trust. We propose a composite trust-based public key management (CTPKM) with the goal of maximizing performance while mitigating security vulnerability.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE 12th International Symposium on Autonomous Decentralized Systems
Date Received: 28-Aug-2016 Conference Date: 25-Mar-2015 Date Published: 28-Mar-2015
Conference Location: Taichung, Taiwan
Paper Title: Trust-Based Task Assignment in Autonomous Service-Oriented Ad Hoc Networks
Authors: Y. Wang; I.R. Chen; J.H. Cho
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2016 IEEE International Workshop on Communications Quality and Reliability (CQR 2016)
Date Received: 28-Aug-2016 Conference Date: 10-May-2016 Date Published:
Conference Location: Stevenson, WA, USA
Paper Title: Trust-based cooperative spectrum sensing against SSDF attacks in distributed cognitive radio networks
Authors: Ji Wang; Ing-Ray Chen; Jeffrey J.P. Tsai; Ding-Chau Wang
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 6th IEEE international conference on Innovative Computing Technology
Date Received: 29-Aug-2016 Conference Date: 24-Aug-2016 Date Published: 29-Aug-2016
Conference Location: Dublin, Ireland
Paper Title: A Hierarchical Cloud Architecture for Integrated Mobility, Service, and Trust Management of Service-Oriented IoT Systems
Authors: J. Guo, I.R. Chen, J.J.P. Tsai, H. Al-Hamadi
Acknowledged Federal Support: **Y**

ACCOMPLISHMENTS

1. Hierarchical Trust Management of COI in Mobile Ad Hoc Networks

We designed and validated a dynamic hierarchical trust management protocol to provide a subjective yet accurate assessment of "trust" of community of interest (COI) mobile nodes in ad hoc networks and demonstrate the utility of the trust protocol with practical Army COI applications, including misbehaving node detection, trust-based survivability management, secure routing, service composition, and task allocation. We validated our dynamic hierarchical trust management designs by a novel model-based analysis technique with simulation validation. Specifically, we developed a mathematical model based on continuous-time semi-Markov stochastic processes (for which the event time may follow any general distribution) to define a COI consisting of a large number of mobile nodes designed to achieve missions in the presence of malicious, erroneous, partly trusted, uncertain and incomplete information in heterogeneous mobile environments. The mathematical model can provide a global view of the system and can serve as the basis for *objective trust* (based on ground truth) evaluation. We compare *objective trust* (based on actual status) against *subjective trust* (obtained as a result of executing our trust protocol) as the basis for iteratively fine-tuning the trust algorithm design so that trust bias, i.e., the difference between *subjective trust* and *objective trust* is minimized. This is achieved by identifying and applying the best trust protocol settings during trust computation, propagation and aggregation. *Adaptive trust management* for application performance maximization is achieved by identifying and applying the best trust protocol settings for trust formation, trust revocation, and trust redemption at runtime. We have overcome two major challenging barriers in this research. One barrier is identifying effective mechanisms with which our dynamic hierarchical trust management protocol can learn from past experiences and adapt to changing environment conditions to minimize trust bias, enhance agility, and maximize application performance. To this, we developed effective and efficient mechanisms including *collaborative filtering* for recommendation filtering, *adaptive filtering* for dynamic weight adjustment of protocol parameters in response to changing conditions, and *table lookup* for dynamically and adaptively applying the best protocol settings identified at static design time. Another barrier is developing and validating a node behavior model for nodes in a mission-oriented COI group in tactical networks. To this, we developed a *node behavior model* that models the tradeoff between altruism vs. selfishness behaviors which can happen in tactical operation scenarios as well as a *context-dependent behavior model* that models the relationship between a node's service behavior and a node's perceived context environment.

This particular line of research resulted in the following publications with an explicit acknowledgment to this grant:

[1] I.R. Chen and J. Guo, "Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection," *28th IEEE International Conference on Advanced Information Networking and Applications (AINA 2014),* Victoria, Canada, May 2014.

[2] I.R. Chen and J. Guo, "Hierarchical Trust Management of Community of Interest Groups in Mobile Ad Hoc Networks," *Ad Hoc Networks,* vol. 33, 2015, pp. 154-167.

[3] I.R. Chen, J. Guo, F. Bao and J.H. Cho, "Trust Management in Mobile Ad Hoc Networks for Bias Minimization and Application Performance Maximization," *Ad Hoc Networks,* vol. 19, August 2014, pp. 59-74.

[4] J.H Cho and I.R. Chen, "On the Tradeoff between Altruism and Selfishness in MANET Trust Management," *Ad Hoc Networks,* vol. 11, Oct. 2013, pp. 2217–2234.

[5] Y. Wang, Y.C. Lu, I.R. Chen, J.H. Cho, A. Swami, and C.T. Lu, "LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks," *6th ASE International Conference on Privacy, Security, Risk and Trust,* Boston, MA, Dec. 2014

[6] Y. Wang, I.R. Chen, J.H. Cho, A. Swami, Y.C. Lu, C.T. Lu, and J.J.P. Tsai, "CATrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks," *IEEE Transactions on Services Computing*, 2017.

We highlight key design concepts (in italic form) developed and covered in the above papers. In [1] [2] we proposed *dynamic hierarchical trust management* for mobile groups in an ad hoc network and applied it to *trust-based misbehaving node detection*. In [3], we proposed and applied the new design concepts of *trust bias minimization* and *application performance maximization* by means of dynamic weight adjustment of protocol parameter settings illustrated with *survivability management* of mobile groups in mobile ad hoc environments. In [4], we developed a *node behavior model* based on altruism vs. selfishness behaviors. Rather than always encouraging altruistic behaviors, we considered the tradeoff between a node's individual welfare (e.g., saving energy to prolong the node lifetime) versus global welfare (e.g., achieving a given mission with sufficient service availability) and identified the best design condition of this behavior model to balance selfish vs. altruistic behaviors. With this behavior model, we demonstrated the utility of *dynamic trust management* for application performance maximization in mobile ad hoc network environments. In

[5][6], we proposed a *context-dependent behavior model* that models the relationship between a node's service behavior and the context environment it is in when the service is requested, resulting in a context-aware trust model called CATrust. The novelty of our design lies in the use of logistic regression to dynamically estimate trustworthiness of a service provider based on its service behavior patterns in response to context environment changes. We demonstrated that CATrust outperforms contemporary P2P trust models in terms of service trust prediction accuracy against collusion recommendation attacks.

2. Adaptive Trust Management for Internet of Things Systems

An Internet of Things (IoT) system aims to connect "things" in both physical world and cyberspace, which raises great challenges to trust management with respect to heterogeneity, scalability, and system dynamics. With support from this ARO grant, we proposed and analyzed the design notion of *adaptive trust management* for IoT systems in which social relationships evolve dynamically among the owners of IoT devices. We considered distributed, centralized, and hierarchically structured IoT systems, all with scalability considerations. For each system, we formally proved the convergence, accuracy, and resiliency properties of our adaptive trust management protocol against malicious attacks. Unlike existing trust protocols for mobile wireless systems designed with wireless communication in mind with monitoring based detection as the main mechanism for trust/reputation assessment, which may not be applicable to an IoT system, our trust management protocol in addition takes dynamically changing social relationships among the owners of devices in an IoT system into account for recommendation filtering. With our adaptive trust management protocol in place, an IoT application can adaptively choose the best trust parameter settings in response to changing conditions such that not only trust assessment is accurate but also the application performance is maximized. We demonstrated the effectiveness of *adaptive trust management* by many real-world IoT applications including service composition & binding, service planning, participatory sensing, environmental monitoring, and health IoT applications.

This particular line of research resulted in the following publications with an explicit acknowledgment to this grant:

[7] I.R. Chen, F. Bao, and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 13, no. 6, Nov-Dec 2016, pp. 684-696.
[8] I.R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, 2016, pp. 482-495.
[9] J. Guo, I.R. Chen, and J.J.P. Tsai, "A Survey of Trust Computation Models for Internet of Things Systems," *Computer Communications*, vol. 97, 2017, pp. 1-14.
[10] J. Guo and I.R. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," *12th IEEE International Conference on Services Computing*, New York, June 2015.
[11] I.R. Chen, J. Guo, and J.J.P. Tsai, "Trust as a Service for SOA-based Internet of Things," *Services Transactions on Internet of Things,* 2017.
[12] J. Guo, I.R. Chen, and J.J.P. Tsai, "A Mobile Cloud Hierarchical Trust Management Protocol for IoT Systems," *5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, April 2017.
[13] J. Guo, I.R. Chen, J.J.P. Tsai, and H. Al-Hamadi, "A Hierarchical Cloud Architecture for Integrated Mobility, Service, and Trust Management of Service-Oriented Internet of Things," *6th IEEE international conference on Innovative Computing Technology (INTECH 2016)*, Dublin, Ireland, 2016.

We highlight key achievements in the above papers. In [7] we proposed and analyzed the design notion of *adaptive trust management* for social Internet of Things (IoT) systems in which social relationships evolve dynamically among the owners of IoT devices. We revealed the design tradeoff between trust convergence vs. trust fluctuation in our *adaptive trust management* protocol design. We proposed a table-lookup method to apply the analysis results dynamically and demonstrate the feasibility of our proposed *adaptive trust management* scheme with two real-world social IoT service composition applications. In [8] we developed adaptive and scalable trust management to support service composition applications in SOA-based IoT systems. We developed a technique based on *distributed collaborative filtering* to select feedback using similarity rating of friendship, social contact, and community of interest relationships as the filter. Further we developed a novel *adaptive filtering* technique to determine the best way to combine direct trust and indirect trust dynamically to minimize convergence time and trust estimation bias in the presence of malicious nodes performing opportunistic service and collusion attacks. We demonstrated the effectiveness of our proposed trust management through service composition application scenarios with a comparative performance analysis against contemporary distributed P2P trust protocols. In [9][10], we developed a classification scheme to classify existing IoT trust computation models based on five design dimensions: *trust composition*, *trust propagation*, *trust aggregation*, *trust update*, and *trust formation*. We analyzed advantages and drawbacks of each dimension's options, and highlighted the effectiveness of defense mechanisms against malicious attacks. We summarized the most and least studied IoT trust computation techniques in the literature and provided insight on the effectiveness of trust computation techniques as applying to IoT systems. We identified gaps in IoT trust computation research and suggested future research directions. In [11], we developed a cloud-based trust management protocol to realize the trust-as-a-service cloud (TaaS) utility for large SOA-based IoT systems. We demonstrated via simulation the superiority of our cloud-based protocol over existing distributed IoT trust protocols in trust convergence, accuracy and resiliency against malicious nodes performing bad-mouthing, ballot-stuffing, and opportunistic service attacks. In [12][13], we proposed a scalable hierarchical cloud architecture for integrated mobility, service, and trust management of service-oriented IoT systems. This architecture supports scalability, reconfigurability, fault tolerance, and resiliency against cloud node failure and network disconnection, and can benefit both network operators and cloud service providers. In particular, we developed a hierarchically structured cloud-based trust protocol to provide trustworthiness assessment of IoT devices in a large scale IoT system. With air pollution detection as an example IoT application, we demonstrate that our cloud-based trust protocol built upon the proposed cloud hierarchy outperforms contemporary distributed IoT trust management protocols.

3. (Add-on.) Trust-based Service Composition and Binding for Tactical Networks with Multiple Objectives

In this research, we proposed a trust-based service composition and service binding protocol for a tactical network where we are concerned with multi-objective optimization (MOO). We formulated the problem of service composition and service binding as a MOO problem such that by dynamically formulating service composition and selecting the right nodes to provide requested services, the tactical network can support concurrent operations while achieving multiple system objectives, such as minimizing the service cost while maximizing the quality of service (QoS) and quality of information (QoI).

This particular line of research resulted in the following publications with an explicit acknowledgment to this grant:

[14] J.H. Cho, Y. Wang, I.R. Chen, K.S. Chan, and A. Swami, "A Survey on Modeling and Optimizing Multi-Objective Systems," *IEEE Communications Surveys and Tutorials*, 2017.

[15] Y. Wang, I.R. Chen, J.H. Cho, K.S. Chan, and A. Swami "Trust-Based Service Composition and Binding with Multi-Objective Optimization in Service-Oriented Ad Hoc Networks," *IEEE Transactions on Services Computing,* 2017.

[16] Y. Wang, I.R. Chen, and J.H. Cho, "Trust-based Service Management of Mobile Devices in Ad Hoc Networks," *8th International Conference on Dependability* (*DEPEND 2015*), Venice, Italy, Aug. 2015.

[17] Y. Wang, I.R. Chen, J.H. Cho, K.S. Chan and A. Swami, "Trust-based Service Composition and Binding for Tactical Networks with Multiple Objectives," *32th IEEE Military Communications Conference (MILCOM 2013),* San Diego, CA, Nov. 2013.

In [14] we conducted a comprehensive survey of the state-of-the-art modeling and solution techniques (trust-based or non-trust-based) to solve multi-objective optimization (MOO) problems. We classified existing approaches based on the types of objectives and investigate main problem domains, critical tradeoffs, and key techniques used in each class. We discussed the overall trends of the existing techniques in terms of application domains, objectives, and techniques, and discussed challenging issues based on the inherent nature of MOO problems. We suggested future work directions in terms of what critical design factors should be considered to design and analyze a system with multiple objectives. In [15][16][17], we applied the design concept of *trust-based application performance optimization* to service composition with MOO goals in military tactical networks. Requested services must be decomposed into more abstract services and then bound; we formulate this as a MOO problem to minimize the service cost, while maximizing the quality of service and quality of information in the service a user receives. The MOO problem is an SP-to-service assignment problem. We developed a multidimensional trust based algorithm to solve the problem. We carried out an extensive suite of simulations to test the relative performance of the proposed trust-based algorithm against a non-trust-based counterpart and an existing single-trust-based beta reputation scheme. Our proposed algorithm effectively filters out malicious nodes exhibiting various attack behaviors by penalizing them with loss of reputation, which ultimately leads to high user satisfaction. Further, our proposed algorithm is efficient with linear runtime complexity while achieving a close-to-optimal solution.

4. (Add-on.) Trust-based Multi-Objective Optimization for Node-to-Task Assignment in Coalition Networks

In military operations, a temporary coalition is often formed to pursue a common goal based on the collaboration of multiple partners who may have their own objectives. The coalition network must attain multiple objectives, under resource constraints and time deadlines. With support from this ARO grant, we developed a trust-based task assignment protocol for a tactical coalition network where we are concerned with multi-objective optimization, namely, maximizing resilience and resource utilization while minimizing delay to task completion. We developed a heuristic coalition formation technique that uses multiple dimensions of trust (i.e., integrity, competence, social connectedness, and reciprocity) to assess trustworthiness of each entity. The proposed scheme enables task leaders to make critical node-to-task assignment decisions based on the tradeoff between risk and trust for maximizing MOO performance.

This particular line of research resulted in the following publications with an explicit acknowledgment to this grant:

[18] Y. Wang, I.R. Chen, J.H. Cho, and J.J.P. Tsai, "Trust-Based Task Assignment with Multi-Objective Optimization in Service-Oriented Ad Hoc Networks," *IEEE Transactions on Network and Service Management,* vol. 14, no. 1, March 2017, pp. 217-232.

[19] Y. Wang, I.R. Chen and J.H. Cho, "Trust-Based Task Assignment in Autonomous Service-Oriented Ad Hoc Networks," *12th IEEE International Symposium on Autonomous Decentralized System*s (*ISADS 2015*), Taichung, Taiwan, March 2015, pp. 71-77.

[20] J.H. Cho, I.R. Chen, Y. Wang, and K.S. Chan, "Trust-based Multi-Objective Optimization for Node-to-Task Assignment in Coalition Networks," *19th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2013), Seoul, Korea,* Dec. 2013, pp. 372-379.

In [18][19][20], we applied the design concept of *trust-based application performance optimization* to task assignment with multiple objective optimization goals in military tactical networks. We considered a mission-driven service-oriented MANET that must handle dynamically arriving tasks to achieve multiple conflicting objectives. We devised a trust-based heuristic algorithm based on auctioning with local knowledge of node status to solve this node-to-task assignment problem with multi-objective optimization (MOO) requirements. Our trust-based heuristic algorithm has a polynomial runtime complexity, rather than an exponential runtime complexity as in existing work, thus allowing dynamic node-to-task assignment to be performed at runtime. It outperforms a non-trust-based counterpart using blacklisting techniques while performing close to the ideal solution quality with perfect knowledge of node status over a wide range of environmental conditions. We conducted extensive sensitivity analysis of the results with respect to key design parameters and alternative trust protocol designs. We also developed a table-lookup method to apply the best trust protocol parameter settings upon detection of dynamically changing environmental conditions to maximize MOO performance.

5. (Add-on.) Adaptive Trust Management in Delay Tolerant Networks

Delay tolerant networks (DTNs) are often encountered in military network environments where end-to-end connectivity is not guaranteed due to frequent disconnection or delay. In this line of research, our objective is to devise and validate adaptive trust management protocols that would allow accurate peer-to-peer trust evaluation in DTN environments while maximizing trust-based application performance in terms of delivery ratio and message delay, without incurring high message or protocol maintenance overhead.

This particular line of research resulted in the following publications with an explicit acknowledgment to this ARO grant:

[21] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, 2014, pp. 1200-1210.

[22] J.H. Cho and I.R. Chen, "PROVEST: Provenance-based Trust Model for Delay Tolerant Networks," *IEEE Transactions on Dependable and Secure Computing,* 2017.

In [21], we proposed and applied *adaptive trust management*, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance, to delay tolerant networks (DTNs) illustrated with *trust-based secure routing* as an application. We designed and validated a trust protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. We performed a comparative analysis of our proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. The results demonstrate that our protocol is able to deal with selfish behaviors and is resilient against trust-related attacks. Furthermore, our trust-based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio. Our trust-based routing protocol operating under identified best settings outperforms Bayesian trust-based routing and PROPHET, and approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead. In [22] we developed a *provenance*-based trust framework called PROVEST that aims to achieve accurate peer-to-peer trust assessment and maximize the delivery of correct messages received by destination nodes while minimizing message delay and communication cost under resource-constrained network environments. PROVEST leverages *provenance* (i.e., the history of ownership of a valued object or information) addressing the interdependency between trustworthiness of information source and information itself. PROVEST takes a data-driven approach to reduce resource consumption in the presence of selfish or malicious nodes while achieving *adaptive trust management*, i.e., estimating a node's trust dynamically in response to changes in the environmental and node conditions. We conducted a comparative performance analysis of PROVEST against existing trust-based and non-trust-based DTN routing protocols to analyze the benefits of PROVEST. We validated PROVEST using a real dataset of DTN mobility traces.

6. (Add-on.) Robust Regression in Adversarial Corruption

The presence of data noise and corruptions recently invokes increasing attention on Robust Least Squares Regression (*RLSR*), which addresses the fundamental problem that learns reliable regression coefficients when response variables can be arbitrarily corrupted. In this line of research, our objective is to handle the following challenges in robust least squares regression concurrently: 1) exact recovery guarantee of regression coefficients 2) difficulty in estimating the corruption ratio parameter; and 3) scalability to massive dataset.

This particular line of research resulted in the following publication:

[22] X. Zhang, L. Zhao, A. Boedihardjo, and C.T. Lu, "Robust Regression via Heuristic Hard Thresholding," 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, August 2017.

In [22], we proposed a novel *robust Least squares regression algorithm* via Heuristic Hard-thresholding (RLHH), that concurrently addresses all the above challenges. Specifically, the algorithm alternately optimizes the regression coefficients and estimates the optimal uncorrupted set via heuristic hard-thresholding without corruption ratio parameter until it converges. The main contributions of our study are summarized as follows: (1) We design an efficient algorithm to address the RLSR problem without parameterizing its corruption. The algorithm RLHH is proposed to recover the regression coefficients and uncorrupted set efficiently. Unlike with a fixed corruption ratio, our method alternately estimates the optimal corruption ratio based on residual errors using optimized regression coefficients in each iteration. (2) We achieve exact recovery guarantees under a mild assumption regarding input variables. We prove that our RLHH algorithm converges at a geometric rate and recovers $\beta*$ exactly under the assumption that the least squares function satisfies both the *Subset Strong Convexity* (SSC) and *Subset Strong Smoothness* (SSS) properties. Specifically, we prove that our heuristic hard thresholding function ensures that the residual of the estimated uncorrupted set in each iteration has a tight upper error bound for the true uncorrupted set. (3) We achieve empirical effectiveness and efficiency. Our proposed algorithm was evaluated with 6 competing methods in synthetic data. The results demonstrate that our approach consistently outperforms existing methods in both regression coefficients and uncorrupted set recovery, delivering a competitive running time.

7. (Add-on.) Multimodal Storytelling via Generative Adversarial Imitation Learning

Deriving event storylines is an effective summarization method to succinctly organize extensive information, which can significantly alleviate the pain of information overload. The critical challenge is the lack of widely recognized definition of storyline metrics. Prior studies have developed various approaches based on different assumptions about users' interests. These works can extract interesting patterns, but their assumptions do not guarantee that the derived patterns will match users' preferences. On the other hand, their exclusiveness of single modality source misses cross-modality information.

This particular line of research resulted in the following publication:

[23] Z. Chen, X. Zhang, A. Boedihardjo, J. Dai, and C.T. Lu, "Multimodal Storytelling via Generative Adversarial

Imitation Learning," 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, August 2017.

In [23], we propose a method, multimodal imitation learning via generative adversarial networks (MIL-GAN), to directly model users' interests as reflected by various data. In particular, the proposed model addresses the critical challenge by imitating users' demonstrated storylines. Our proposed model is designed to learn the reward patterns given user-provided storylines and then applies the learned policy to unseen data. The proposed approach is demonstrated to be capable of acquiring the user's implicit intent and outperforming competing methods by a substantial margin with a user study. The main contributions of our study are summarized as follows: (1) We propose an imitation learning method for storytelling: To avoid the difficulty in designing reward function for storytelling, we enforce generative adversarial model on imitation learning. Using this learning strategy, the model can robustly model latent connectivity patterns. (2) We design a multimodal model integrated with GAN based imitation learning: Inspired by human's ability to link multiple entities through visual similarity, we propose a multimodal method across textual and visual modality with imitation learning. Our model learns reward functions from these two modalities and their correlation. (3) We create a benchmark dataset for multimodal imitation storytelling: A new multimodal storytelling dataset is collected from multiple attacks and civil unrest events. Under several selected topics, storylines are manually extracted and validated. Both texts and images are included in our dataset.